

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:

Apple iPhone, red in color with “(PRODUCT)RED”
inscribed on the back, seized on March 11, 2021 by
Allegheny County Police and currently stored at the
Allegheny County Police Headquarters

Apple iPhone, Model A1660 FCC ID: BCG-
E3085A IC: 579C-E3085A, seized on March 11,
2021 by Allegheny County Police and currently
stored at the Allegheny County Police Headquarters

Magistrate No. 21-623

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Detective Judson Ekis, being duly sworn, depose and state that:

INTRODUCTION AND AGENT BACKGROUND

1. This Affidavit is made in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for the issuance of a search warrant authorizing the search of cellular telephones currently in law enforcement custody as described below and in Attachment A, and the extraction from that property of the electronically stored information described in Attachment B.

2. I am a Detective with the Allegheny County Police Department having been so since 2006. I have been a narcotics detective for 8 years and have been deputized Federally under Title 21 for approximately two years. During this time, I have investigated numerous drug related offenses. Your affiant is authorized to investigate violations of Title 21 United States Code and related provisions. As such I am familiar with the way in which individuals involved in illegal drug trafficking unlawful firearms possession use cellular telephones and the evidence that can be obtained from cellular telephones of individuals involved in that illegal activity.

3. The information contained herein is based upon my own personal investigation,

observations, and knowledge as well as upon the investigation, personal observations, and knowledge of other law enforcement officers with whom I have discussed this case. Because this Affidavit is being submitted for the limited purpose of establishing probable cause in support of a search warrant, I have not included every item of evidence or piece of information known to me; rather, I have included only those facts necessary to establish probable cause.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. This Application and Affidavit are being submitted in support of a search warrant for the following electronic devices, which are currently logged into Allegheny County Police Headquarters Evidence under Property Control Number: 21-0296 Item: AC

- a. Apple iPhone, red in color with “(PRODUCT)^{RED}” inscribed on back (hereinafter **TELEPHONE 1**).
- b. Apple iPhone, Model A1660 FCC ID: BCG-E3085A IC: 579C-E3085A (hereinafter **TELEPHONE 2**).

5. Investigators, including your Affiant, believe the records and other information contained within **TELEPHONE 1** and **TELEPHONE 2** contain evidence of violations of Title 21, United States Code, Sections 841 and 846, which make it unlawful for individuals to possess with intent to distribute and distribute controlled substances or conspire to do the same, and Title 18, United States Code, Sections 922 and 924, which make it unlawful for certain individuals to possess firearms and prohibits the possession of firearms during and in relation to crimes of violence and in furtherance of drug trafficking activity (hereinafter the **TARGET OFFENSES**).

6. The applied-for warrants would authorize the forensic search of **TELEPHONE 1** and **TELEPHONE 2** for the purpose of identifying electronically stored data particularly described in Attachment B.

FACTS RELATING TO PROBABLE CAUSE

7. On March 11, 2021, detectives with the Allegheny County Police Department arrived in the area of 310 Comrie Avenue, Second Floor Apartment, Braddock, PA 15104 for the purpose of executing a search warrant.

8. Prior to the execution of a search warrant on that location, detectives with the Allegheny County Police Department intercepted Jared Thomas (“THOMAS”) as he was approaching a Lincoln SUV. THOMAS was found to be in possession of a baggie of crack-cocaine. THOMAS was mirandized and advised detectives there was additional drug evidence inside of the target location.

9. Detectives proceeded to the target location and were required to use force to gain entry because Catherine Strong (“STRONG”) refused to open the door for the detectives. Once entry was made into the residence, detectives located STRONG. STRONG was holding TELEPHONE 1 in her hand. A thorough search of the residence revealed that STRONG was in close proximity to an unsecured bag holding 9 “bricks” of heroin, 29 bundles of heroin, and approximately 10 grams of field-tested fentanyl.

10. Additionally, detectives located baggies of crack cocaine (approximately 139 grams) inside of a locked bedroom and 67 ecstasy pills from a purse located inside of STRONG’s reported bedroom. TELEPHONE 2 was also located in the bedroom containing the purse.

11. Your Affiant is aware through both training as well as experience gained through multiple narcotics investigations, the targets of those narcotics investigations utilize cellular telephones to not only arrange meetings with their drug customers but also speak with fellow co-conspirators as well as their drug sources of supply. Your Affiant is also aware that these targets also utilize multiple cellular telephones at one time in an effort to not only thwart detection by law

enforcement but also to compartmentalize their drug trafficking customers to one phone, their co-conspirators to another phone, and their drug source of supply to yet another phone.

12. Based upon my training and experience, I am aware that it is generally a common practice for drug traffickers to store the names and phone numbers of drug customers and photographs and video detailing illegal activities in cellular telephones. Because drug traffickers in many instances will “front” (that is, sell on consignment) controlled substances to their clients, and/or will be “fronted” controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep “pay and owe” records to show balances due for drugs sold in the past (“pay”) and for payments expected (“owe”) as to the trafficker’s supplier(s) and the trafficker’s dealer(s). Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their drug trafficking business.

13. Members of Drug Trafficking Organizations (DTO) often take group photographs with other enterprise members posing with paraphernalia, money and/or drugs. Many cellular telephones, including **TELEPHONE 1** and **TELEPHONE 2**, have a camera feature that is readily capable of capturing and storing these group photos. In my experience, the phones of individuals who illegally possess firearms often contain evidence of unlawful firearm possession in the form of text messages, e-mails, and social media posts. It has also been my experience that such phones often contain information regarding how an unlawful possessor acquired his firearm.

14. Members of DTOs often store each other’s phone numbers and contact information in the directories of their cellular phones.

15. Based on my experience and familiarity with cellular telephones, I am aware that the telephones have voicemail and telephone directory features, as well as camera features which allow the user to take photographs and store them in the cellular phone's memory card. Based on my experience and training, statements by other law enforcement officers, and personal observations, I know that because of the storage capacity of cellular telephones, the portability of cellular telephones, the ease with which information stored on a cellular telephone may be accessed and/or organized, and the need for frequent communication in arranging narcotics transactions, cellular telephones are frequently used by individuals involved in drug trafficking. In particular, I and other law enforcement officers have found that information frequently maintained on cellular telephones includes the contact numbers of other co-conspirators, contact numbers for narcotics customers and stored photographs of DTO activities. This evidence will come in the form of caller identification information, call log information, telephone numbers, address information, or other identification information, as well as opened and unopened voicemail and/or text messages, photographs, videos and information about access to the Internet.

16. Members of DTOs routinely use multiple physical phones in succession as one breaks or the DTO feels that the number associated with the phone is compromised to Law Enforcement. The physical phone may no longer be an active communicative device, however many times, these old phones are not discarded as they possess value to the DTO. The replaced device contains within it the contact information for drug customers of the DTO, and many times these phones are maintained as digital phone books should the new active phone become unusable or unavailable. Furthermore, these replaced phones are commonly kept in a relatively accessible location where either all or select members of the DTO can access the information within should it become necessary. As stated above, members of DTOs routinely take photographs and or

memorialize other information of evidentiary value within these replaced phones. As such, it is common to recover a multitude of otherwise inactive phones especially at locations central to or important to the DTO. Additionally, your affiant knows that persons who are legally prohibited from the purchase and possession of firearms acquire firearms through unlawful means. In order to do so the solicitation and transaction thereof is often conducted via digital media devices and the conversations, pictures and specifics of the transaction are often stored within cellular devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

17. As described above and in Attachment A, this Application seeks permission to search **TELEPHONE 1** and **TELEPHONE 2** for records that might be found on **TELEPHONE 1** and **TELEPHONE 2** which will provide evidence of violations of the **TARGET OFFENSES**.

18. One form in which the records might be found is data stored on a cellular telephone.

19. Based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

20. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

21. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, an electronic device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

22. Wholly apart from user-generated files, electronic device storage media—in particular, electronic devices’ internal hard drives—contain electronic evidence of how an electronic device has been used, what it has been used for, where it was located, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Electronic device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

23. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments,

and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.


26. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement’s possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

27. Based upon the foregoing, you Affiant submits that there is probable cause to believe TELEPHONE 1 and **TELEPHONE 2** contains information related to the **TARGET OFFENSES**, which there is probable cause to believe have been violated by Catherine STRONG.

/s/ Judson Ekis
Det. Judson Ekis
Allegheny County Police

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 19th day of March, 2021.



HONORABLE LISA PUPO LENIHAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Devices to be Searched

1. TELEPHONE 1

- b. Apple iPhone, red in color with “(PRODUCT)^{RED}”, and currently located at the Allegheny County Police headquarters, referred to as **TELEPHONE 1**.

This device is currently in the custody the Allegheny County Police Department.

2. TELEPHONE 2

- a. Apple iPhone, Model A1660 FCC ID: BCG-E3085A IC: 579C-E3085A, and currently located at the Allegheny County Police headquarters, referred to as **TELEPHONE 2**. This device is currently in the custody the Allegheny County Police Department.

ATTACHMENT B

Records and Other Information to Be Seized

1. All records, information, and items evidencing who used the device and/or when and/or from where, as well as evidence of violations of the following statutes including but not limited to 21 U.S.C. §§ 841, 846 and 18 U.S.C. §§ 922, 924, and on **TELEPHONE 1** and **TELEPHONE 2**, including:

- a. incoming and outgoing call and text message logs,
- b. contact lists,
- c. photo and video galleries,
- d. sent and received text messages,
- e. online searches and sites viewed via the internet,
- f. online or electronic communications sent and received, including email, chat, and instant messages,
- g. sent and received audio files,
- h. navigation, mapping, and GPS files,
- i. telephone settings, including speed dial numbers and the telephone number for **TELEPHONE 1** and **TELEPHONE 2** and related identifying information such as the ESN for **TELEPHONE 1** and **TELEPHONE 2**,
- j. call forwarding information,
- k. messages drafted but not sent, and
- l. voice messages.

2. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. However, no real-time communications will be intercepted and searched during execution of the search warrant.

3. In searching **TELEPHONE 1** and **TELEPHONE 2**, investigating officers and agents may examine all of the data contained in **TELEPHONE 1** and **TELEPHONE 2** to view

the precise contents and determine whether **TELEPHONE 1** and **TELEPHONE 2** and/or its data falls within the items to be seized as set forth above. In addition, they may search for and attempt to recover “deleted,” “hidden” or encrypted data to determine whether the data falls within the list of items to be seized as set forth above.